

# SETS OF LENGTHS OF POWERS OF A VARIABLE

RICHARD BELSHOFF, DANIEL KLINE AND MARK W. ROGERS

**ABSTRACT.** A positive integer  $k$  is a *length* of a polynomial if that polynomial factors into a product of  $k$  irreducible polynomials. We find the set of lengths of polynomials of the form  $x^n$  in  $R[x]$ , where  $(R, \mathfrak{m})$  is an Artinian local ring with  $\mathfrak{m}^2 = 0$ .

**1. Introduction.** In this paper we study the non-uniqueness of factorizations of  $x^n$  in  $R[x]$ , where  $(R, \mathfrak{m})$  is a commutative Artinian local ring with identity, with the added restriction that  $\mathfrak{m}^2 = 0$ . For example,  $R$  could be the ring  $\mathbb{Z}/p^2\mathbb{Z} = \mathbb{Z}_{p^2}$  where  $p$  is prime.

**Example 1.1.** Consider the following factorizations of  $x^6$  in  $\mathbb{Z}_9[x]$ .

- (1)  $x^6 = x \cdot x \cdot x \cdot x \cdot x \cdot x$
- (2)  $x^6 = x \cdot x \cdot (x^2 + 3) \cdot (x^2 - 3)$
- (3)  $x^6 = (x^2 + 3) \cdot (x^2 + 3) \cdot (x^2 + 3)$
- (4)  $x^6 = (x^3 + 3) \cdot (x^3 - 3)$

The first factorization expresses  $x^6$  in the usual way as a product of 6 irreducible polynomials; for this reason, we say that 6 is a *length* of  $x^6$ , and if  $R$  were a unique factorization domain, this would be the only length of  $x^6$ . However, the remaining factorizations show that 4, 3, and 2 are lengths of  $x^6$ . As we will later see, these are all of the lengths of  $x^6$ , and we write  $L(x^6) = \{2, 3, 4, 6\}$ . In general, the set of lengths of  $x^n$  in  $\mathbb{Z}_{p^2}[x]$  depends on whether  $p = 2$  or  $p$  is an odd prime. For example, in  $\mathbb{Z}_4[x]$ ,  $L(x^6) = \{2, 4, 6\}$ .

Our goal in this paper is the collection of results Proposition 4.6, Lemma 4.10, and Theorem 4.14, which completely determine  $L(x^n)$  over Artinian local rings that are not fields but for which the square of the maximal ideal is zero. The result depends on whether  $n$  is even or odd, and whether the cardinality of  $R$  is 4 or not (there are only two such rings with cardinality 4). For example, if  $n$  is an even integer and the cardinality of  $R$  is greater than 4, we show that  $L(x^n) = \{2, 3, 4, 5, \dots, n-2\} \cup \{n\}$ , as we saw above for  $n = 6$ .

For a recent survey of sets of lengths, we refer the reader to the recent paper [G] by Alfred Geroldinger.

**2. Preliminaries.** For the rest of this paper, unless otherwise specified,  $(R, \mathfrak{m})$  is a commutative Artinian local ring identity, having unique maximal ideal  $\mathfrak{m} \neq 0$  and residue field  $\overline{R} = R/\mathfrak{m}$ ;  $R[x]$  is the polynomial ring in the variable  $x$  with coefficients in  $R$ . The concept of an *irreducible element* is usually defined only for integral domains. For rings with zero-divisors, several different notions of irreducible have been proposed ([A1], [A2], [A3].) Our definition of irreducible will be the usual one, i.e., the one that is used when  $R$  is an integral domain. We begin by recalling this and a few other definitions and equivalences. Let  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$  denote a polynomial of degree  $d$  in  $R[x]$ .

- The polynomial  $f(x)$  is a *unit* if  $a_0$  is a unit and  $a_i \in \mathfrak{m}$  for all  $i > 0$ .

---

2000 AMS *Mathematics subject classification.* Primary 13A05; Secondary 13E10.  
*Keywords and phrases.* non-unique factorization, Artinian local ring, polynomial.  
 Received by the editors July 11, 2016.

- The polynomial  $f(x)$  is a *zero divisor* if each  $a_i \in \mathfrak{m}$ . Note that any multiple of a zero divisor is a zero divisor.
- The polynomial  $f(x)$  is *regular* if  $f(x)$  is not a zero divisor. Note that if a product is regular, so is each factor.
- The nonunit polynomial  $f(x)$  is *irreducible* if  $f(x) = g(x)h(x)$  implies  $g(x)$  or  $h(x)$  is a unit.
- The *order* of the polynomial  $f(x)$  (denoted  $\text{ord}(f)$ ) is the least  $i$  such that  $a_i \neq 0$ .
- By  $\overline{f}(x)$  we mean the image of  $f(x)$  in  $\overline{R}[x]$ .

The following proposition is proved by B. R. McDonald ([M], Theorem XIII.6) for finite rings. The result generalizes to the case where  $R$  is any Artinian local ring. We will need this result in Lemma 4.3.

**Proposition 2.1.** *Every regular polynomial  $f$  in  $R[x]$  is representable as  $f = uf^*$  where  $u$  is a unit of  $R[x]$  and  $f^*$  is a monic polynomial of  $R[x]$ . Also,  $\deg(f^*) = \deg(\overline{f})$ .*

The following simple corollary allows us to assume that irreducible factors of a monic polynomial are themselves monic, and thus nonconstant. We use this corollary implicitly throughout the paper.

**Corollary 2.2.** *If  $f$  is a monic polynomial in  $R[x]$  such that  $f = f_1 f_2 \cdots f_k$  for some polynomials  $f_1, f_2, \dots, f_k$  then there are monic polynomials  $f_1^*, f_2^*, \dots, f_k^*$  such that  $f = f_1^* f_2^* \cdots f_k^*$ . If each  $f_i$  is irreducible, then each  $f_i^*$  is irreducible (and nonconstant).*

*Proof.* Since the product  $f_1 \cdots f_k$  is regular, so is each  $f_i$ . By Proposition 2.1, each  $f_i = u_i f_i^*$  for some unit  $u_i$  and some monic polynomial  $f_i^*$ . Since  $f = (u_1 \cdots u_k) f_1^* \cdots f_k^*$  and  $f$  and  $f_1^* \cdots f_k^*$  are both monic, the leading coefficient of the unit  $u_1 \cdots u_k$  is 1. The only unit with this property is 1, so  $f = f_1^* f_2^* \cdots f_k^*$ . If each  $f_i$  is irreducible, then so are the associates  $f_i^*$ ; they cannot be constant, since the only monic constant is 1, and units aren't considered irreducible.  $\square$

**3. Generalized Eisenstein Polynomials.** We begin by showing that while factorization in  $R[x]$  may be non-unique, it is at least possible. We remind the reader that  $(R, \mathfrak{m})$  is an Artinian local ring with  $\mathfrak{m} \neq 0$ .

**Proposition 3.1.** *Every polynomial of positive degree in  $R[x]$  that is not a unit can be factored into a product of irreducible polynomials.*

*Proof.* Suppose  $f(x) = a_d x^d + \cdots + a_1 x + a_0$  is a zero divisor of  $R[x]$ . Then, for  $0 \leq k \leq d$ , we have  $a_k \in \mathfrak{m}$ , hence  $a_k$  is nilpotent. Now

$$1 - f(x) = -a_d x^d - \cdots - a_1 x + (1 - a_0)$$

and  $1 - a_0$  is a unit. Therefore  $1 - f(x)$  is a unit of  $R[x]$ .

This shows that the ring  $R[x]$  has *harmless zero-divisors* using the terminology of Frei-Frisch [FF, Definition 2.3]. Now the result follows from [FF, Lemma 2.8].  $\square$

**Definition 3.2.** A *generalized Eisenstein polynomial* (abbreviated *GE polynomial*) is a non-constant monic polynomial  $f(x) = x^d + f_{d-1}x^{d-1} + \cdots + f_1x + f_0$  with the property that  $f_i \in \mathfrak{m}$  for each  $i = 0, \dots, d-1$ . Equivalently,  $f(x)$  is a GE polynomial if  $f(x)$  is non-constant, monic and  $\overline{f}(x) = x^d$  in  $\overline{R}[x]$ , where  $d = \deg f$ .

We note that  $x^n$  is a GE polynomial for any positive integer  $n$ .

**Lemma 3.3.** *Let  $f$  and  $g$  be monic, nonconstant polynomials in  $R[x]$ . Then  $fg$  is a GE polynomial if and only if both  $f$  and  $g$  are GE polynomials.*

*Proof.* Assume both  $f$  and  $g$  are GE polynomials; then  $\overline{f} = x^k$  and  $\overline{g} = x^\ell$  where  $k$  and  $\ell$  are the degrees of  $f$  and  $g$ . Thus  $x^{k+\ell} = \overline{fg} = \overline{f}\overline{g}$ , showing that  $fg$  is a GE polynomial.

Conversely, if  $f$  and  $g$  are monic of degrees  $k$  and  $\ell$  respectively, then  $\overline{fg} = \overline{f}\overline{g} = x^{k+\ell}$  since  $fg$  is a GE polynomial. Since  $\overline{R}[x]$  is a UFD, it follows easily that  $\overline{f} = x^k$  and  $\overline{g} = x^\ell$ . Therefore both  $f$  and  $g$  are GE polynomials.  $\square$

The next theorem is the reason for our terminology “generalized Eisenstein polynomial.”

**Theorem 3.4.** *If  $f$  is a GE polynomial in  $R[x]$  whose constant term is in  $\mathfrak{m} \setminus \mathfrak{m}^2$ , then  $f$  is irreducible.*

*Proof.* Suppose by way of contradiction that there are two polynomials  $g, h$  with  $f = gh$ . By Corollary 2.2,  $f = g^*h^*$  for some monic polynomials  $g^*, h^*$ . By Lemma 3.3, either  $g^*$  and  $h^*$  are GE polynomials, or one of them is constant. If one of them is constant then it is a unit, and the proof is complete. If both were nonconstant, then since they are GE polynomials, the product of their constant terms would be in  $\mathfrak{m}^2$ , and this would contradict the assumption on the constant term of  $f$ .  $\square$

**Corollary 3.5.** *Suppose  $\mathfrak{m}^2 = 0$ . If  $f$  is a GE polynomial in  $R[x]$  with degree at least two, then  $f$  is irreducible if and only if  $f$  has a nonzero constant term.*

*Proof.* If  $f$  is a GE polynomial with a nonzero constant term, then the constant term is in  $\mathfrak{m} \setminus \mathfrak{m}^2$  since  $\mathfrak{m}^2 = 0$ . According to Theorem 3.4,  $f$  is irreducible.

If the constant term of  $f$  is zero then

$$f = x^d + a_{d-1}x^{d-1} + \cdots + a_jx^j = x(x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_jx^{j-1})$$

where  $d \geq 2$  and  $1 \leq j \leq d$ . The factorization displayed above is a factorization into a product of two non-units, since  $a_j \in \mathfrak{m}$ . Therefore, if the constant term of  $f$  is zero, then  $f$  is reducible.  $\square$

**Remark 3.6.** Let  $(R, \mathfrak{m})$  be a finite local ring such that  $\mathfrak{m}^2 = 0$  and let  $k = |\mathfrak{m}|$ . By Corollary 3.5, the number of irreducible GE polynomials of degree 2 in  $R[x]$  is exactly  $k(k-1)$ . We will use this remark later in Lemma 4.10.

The central idea of the following proof for the case  $k = 2$  was inspired by the computations done at the start of [FF].

**Proposition 3.7.** *Suppose  $\mathfrak{m}^2 = 0$ . If  $k \geq 2$  and  $f_1, f_2, \dots, f_k$  are GE polynomials in  $R[x]$  with  $\deg(f_i) = d_i$  and  $d_1 \geq d_2 \geq \cdots \geq d_k$  then there is a GE polynomial  $h$  of degree  $d_1$  such that  $f_1 f_2 \cdots f_k = h x^{d_2 + d_3 + \cdots + d_k}$ . If, furthermore,  $f_1$  is irreducible and  $d_1 > d_2$ , then  $h$  is irreducible and  $\text{ord}(\prod_{i=1}^k f_i) = \sum_{i=2}^k d_i$ .*

*Proof.* We use induction on  $k$ . Suppose  $k = 2$ . We have  $f_1 = x^{d_1} + \tilde{f}_1$  and  $f_2 = x^{d_2} + \tilde{f}_2$  where  $\tilde{f}_1, \tilde{f}_2 \in \mathfrak{m}[x]$  have degrees less than  $d_1, d_2$ , respectively. Therefore  $f_1 f_2 = (x^{d_1} + \tilde{f}_1)(x^{d_2} + \tilde{f}_2) =$

$x^{d_1+d_2} + x^{d_1}\tilde{f}_2 + x^{d_2}\tilde{f}_1 + \tilde{f}_1\tilde{f}_2$ . Since  $\mathfrak{m}^2 = 0$  we have  $\tilde{f}_1\tilde{f}_2 = 0$ , so

$$\begin{aligned} f_1f_2 &= x^{d_1+d_2} + x^{d_1}\tilde{f}_2 + x^{d_2}\tilde{f}_1 \\ &= (x^{d_1} + x^{d_1-d_2}\tilde{f}_2 + \tilde{f}_1)x^{d_2} \end{aligned}$$

and the polynomial  $h = x^{d_1} + x^{d_1-d_2}\tilde{f}_2 + \tilde{f}_1$  is a GE polynomial of degree  $d_1$ . If, furthermore,  $f_1$  is irreducible and  $d_1 > d_2$ , then  $h$  is irreducible by Lemma 3.5, since  $h$  and  $f_1$  have the same constant term. Finally, because  $\tilde{f}_1$  has a nonzero constant term, we have  $\text{ord}(f_1f_2) = d_2$ .

Now suppose  $k \geq 2$  and assume  $f_1 \cdots f_k = x^{d_2+\cdots+d_k}h_1$  where  $h_1$  is a GE polynomial with  $\deg(h_1) = d_1$ , and if  $f_1$  is irreducible with  $d_1 > d_2$ , then  $h_1$  is irreducible. Then

$$\begin{aligned} \prod_{i=1}^{k+1} f_i &= f_1 \cdots f_k f_{k+1} \\ &= (h_1 x^{d_2+\cdots+d_k}) f_{k+1} \\ &= x^{d_2+\cdots+d_k} (h_1 f_{k+1}) \\ &= x^{d_2+\cdots+d_k} (h x^{d_{k+1}}) \end{aligned}$$

for some GE polynomial  $h$  of degree  $d_1$  by the  $k = 2$  case, and if  $f_1$  is irreducible with  $d_1 > d_2$ , then  $h$  is irreducible. Therefore  $\prod_{i=1}^{k+1} f_i = h x^{d_2+\cdots+d_k+d_{k+1}}$ . Furthermore, if  $f_1$  is irreducible with  $d_1 > d_2$ , then  $h$  is irreducible, and so it has a nonzero constant term. Therefore  $\text{ord}\left(\prod_{i=1}^{k+1} f_i\right) = d_2 + \cdots + d_k + d_{k+1}$ . This completes the proof by induction.  $\square$

**4. Sets of Lengths of  $x^n$ .** We begin with the definition of the *set of lengths* of an element.

**Definition 4.1.** Let  $R$  be a commutative Artinian local ring with identity and let  $f \in R[x]$ . We say that a positive integer  $n$  is a **length** of  $f$  if  $f$  factors into a product of  $n$  irreducible polynomials in  $R[x]$ . We define the set

$$L(f) = \{n \mid n \text{ is a length of } f\}$$

to be the **set of lengths of  $f$** .

**Remark 4.2.** To say that  $1 \in L(f)$  means precisely that  $f$  is irreducible, and in this case  $L(f) = \{1\}$ . If  $R$  is a unique factorization domain, then  $L(f)$  is a singleton for any polynomial  $f \in R[x]$ . Of course  $n \in L(x^n)$ , and if  $R$  is a UFD then  $L(x^n) = \{n\}$ .

A regular polynomial of degree  $n$  cannot have length greater than  $n$ , according to the next lemma. In fact, after we establish the next three lemmas, we will be able to determine the set of lengths of  $x^n$  for  $n \leq 5$ .

**Lemma 4.3.** *If  $f$  is a regular polynomial in  $R[x]$  of degree  $n$ , then  $L(f) \subseteq \{1, 2, \dots, n\}$ .*

*Proof.* If  $f$  is a unit, then  $L(f) = \emptyset$  since irreducibles aren't units and a product of nonunits can't be a unit; now assume  $f$  is not a unit. Suppose  $k \in L(f)$ ; then there are irreducible polynomials  $f_1, \dots, f_k$  in  $R[x]$  such that  $f = f_1 \cdots f_k$ . Each  $f_i$  must be regular, since  $f$  is, and thus each  $f_i$  has positive degree, since the only regular constants are units. For each  $i = 1, \dots, k$ , we have  $f_i = u_i f_i^*$  for some unit  $u_i$  and some monic  $f_i^*$  in  $R[x]$ , by Proposition 2.1; since  $f_i$  is not a unit,  $f_i^*$  has positive degree. We have  $f = f_1 \cdots f_k = u_1 \cdots u_k f_1^* \cdots f_k^*$  and thus  $k \leq \sum_{i=1}^k \deg(f_i^*) \leq \deg(u_1 \cdots u_k f_1^* \cdots f_k^*) = \deg(f) = n$ .  $\square$

The assumption that  $f$  is a regular polynomial is necessary in Lemma 4.3: If  $R = \mathbb{Z}_4$  then the constant polynomial  $2 \in R[x]$  is irreducible. Hence for the polynomial  $f = 2x$  of degree 1 we have  $2 \in L(f)$ .

**Lemma 4.4.** *Suppose  $\mathfrak{m}^2 = 0$ . If  $n$  is a positive integer then  $n - 1 \notin L(x^n)$ , and if  $n$  is odd then  $2 \notin L(x^n)$ .*

*Proof.* We prove the second part first. Suppose, to get a contradiction, that  $2 \in L(x^n)$  for some odd positive integer  $n$ . By Lemma 4.3 we must have  $n \geq 3$ ; thus there are irreducible nonconstant monic polynomials  $f$  and  $g$  such that  $x^n = fg$ . By Lemma 3.3, both  $f$  and  $g$  are GE polynomials. Since  $n$  is odd,  $\deg(f) \neq \deg(g)$ , so without loss of generality we assume  $\deg(f) > \deg(g)$ . By Proposition 3.7 there is an irreducible GE polynomial  $h$  such that  $x^n = fg = hx^{\deg(g)}$ , so  $n = \text{ord}(x^n) = \text{ord}(fg) = \deg(g) = n - \deg(f)$ , contradicting  $f$  nonconstant. This shows  $2 \notin L(x^n)$  if  $n$  is odd.

Now we prove the first part. Since  $x^2$  is reducible,  $1 \notin L(x^2)$ . We have just shown  $2 \notin L(x^3)$ . Suppose, to get a contradiction,  $n - 1 \in L(x^n)$  for some integer  $n \geq 4$ ; then there are irreducible, nonconstant, monic GE polynomials  $f_1, f_2, \dots, f_{n-1}$  such that  $x^n = f_1 f_2 \cdots f_{n-1}$ . Since  $\deg(f_1 f_2 \cdots f_{n-1}) = n$ , exactly one  $f_i$  has degree 2 and the rest are linear. Without loss of generality, assume polynomials  $f_2$  through  $f_{n-1}$  are linear and  $f_1$  has degree two. By Proposition 3.7,  $f_2 \cdots f_{n-1} = hx^{n-3}$  where  $h$  is a linear GE polynomial. Thus  $x^n = f_1 hx^{n-3}$ , which implies  $x^3 = f_1 h$ . This is a contradiction, since if  $x^3 = f_1 h$  then  $2 \in L(x^3)$ . Therefore  $n - 1 \notin L(x^n)$   $\square$

**Lemma 4.5.** *Suppose  $\mathfrak{m}^2 = 0$ . Let  $q$  be an irreducible GE polynomial in  $R[x]$ . For any integer  $n \geq 2$ ,*

- (1) *If  $n$  is even, then  $\{2, 4, 6, \dots, n - 2, n\} \subseteq L(q^n)$ .*
- (2) *If  $n$  is odd, then  $\{3, 5, 7, \dots, n - 2, n\} \subseteq L(q^n)$ .*

*Proof.* Suppose  $n$  is even. Since  $q$  is irreducible,  $n \in L(q^n)$ . Let  $k$  be any even integer such that  $2 \leq k < n$ ; we will find a factorization of  $q^n$  with length  $k$ . Let  $m$  be any nonzero element of the maximal ideal  $\mathfrak{m}$  and consider the factorization

$$(q^{\frac{n-k+2}{2}} + m)(q^{\frac{n-k+2}{2}} - m) = q^{n-k+2} \quad (4.1)$$

Since  $n - k \geq 2$ ,  $\frac{n-k+2}{2} \geq 2$ , hence  $q^{\frac{n-k+2}{2}}$  is a reducible GE polynomial; by Corollary 3.5,  $q^{\frac{n-k+2}{2}}$  has constant 0, so  $q^{\frac{n-k+2}{2}} + m$  is irreducible. Similarly  $q^{\frac{n-k+2}{2}} - m$  is also irreducible. Multiplying both sides of equation (4.1) by  $q^{k-2}$  yields  $q^{k-2}(q^{\frac{n-k+2}{2}} + m)(q^{\frac{n-k+2}{2}} - m) = q^n$ . Hence we have a product of  $k$  irreducible factors equal to  $q^n$  for any even  $k$  such that  $2 \leq k < n$ . Therefore,  $\{2, 4, 6, \dots, n - 2, n\} \subseteq L(q^n)$ .

If  $n$  is odd, the proof follows the same argument and factorization as above, except this time  $n$  and  $k$  are both odd integers.  $\square$

**Proposition 4.6.** *Suppose  $\mathfrak{m}^2 = 0$ . In  $R[x]$  we have*

$$L(x) = \{1\} \quad L(x^2) = \{2\} \quad L(x^3) = \{3\} \quad L(x^4) = \{2, 4\} \quad L(x^5) = \{3, 5\}$$

*Proof.* This follows directly from Lemmas 4.3, 4.4, and 4.5.  $\square$

We now proceed to find the set of lengths of  $x^6$ . By Lemmas 4.3, 4.4, and 4.5 we have

$$\{2, 4, 6\} \subseteq L(x^6) \subseteq \{2, 3, 4, 6\}.$$

It remains to determine if  $3 \in L(x^6)$ ; this depends on whether  $|R| > 4$  or  $|R| = 4$  as we will see in Lemma 4.10 below.

We first establish some general results about local rings of cardinality 4.

**Proposition 4.7.** *Let  $(R, \mathfrak{m})$  be any local ring. The following are equivalent.*

- (1)  $\text{char}(R/\mathfrak{m}) = 2$
- (2)  $2 \in \mathfrak{m}$

*If  $\mathfrak{m} \neq 0$  but  $\mathfrak{m}^2 = 0$ , then (1) and (2) are equivalent to*

- (3)  $2\mathfrak{m} = 0$

*Proof.* We have  $\text{char}(R/\mathfrak{m}) = 2$  if and only if  $\bar{1} + \bar{1} = \bar{2} = \bar{0}$  in  $R/\mathfrak{m}$  if and only if  $2 \in \mathfrak{m}$ . Now assume  $\mathfrak{m} \neq 0$  but  $\mathfrak{m}^2 = 0$ . For (2) implies (3), given any  $m \in \mathfrak{m}$ , we have  $2m \in \mathfrak{m}^2 = 0$ . Conversely, if  $2\mathfrak{m} = 0$  then 2 is not a unit (since  $\mathfrak{m} \neq 0$ ), so  $2 \in \mathfrak{m}$ .  $\square$

**Proposition 4.8.** *Let  $(R, \mathfrak{m})$  be any local ring. If  $|\mathfrak{m}| = 2$ , then  $|R| = 4$ .*

*Proof.* Since  $R = R^\times \cup \mathfrak{m}$ , the disjoint union of the units  $R^\times$  and the maximal ideal  $\mathfrak{m}$ , it suffices to show that  $R$  has exactly two units. Suppose  $\mathfrak{m} = \{0, t\}$ . If the only unit of  $R$  is 1, then  $R$  is a ring with three elements and is thus isomorphic to  $\mathbb{Z}_3$ , contradicting  $|\mathfrak{m}| = 2$ . Therefore there exists a unit  $u \neq 1$  in  $R$ ; we show  $u = t + 1$ . Since  $ut \in \mathfrak{m}$ , either  $ut = 0$  or  $ut = t$ . The first case is impossible since  $t \neq 0$ . In the second case  $t(u - 1) = 0$  and hence  $u - 1 \in \mathfrak{m}$ . This implies  $u - 1 = t$  so  $u = t + 1$ . This shows that  $R = \{0, 1, t, t + 1\}$ , a ring with four elements.  $\square$

**Remark 4.9.** It is known ([M, Exercise I.4, p.4]) that if  $R$  is any ring with four elements, then  $R$  must be isomorphic to one of the following:  $\mathbb{Z}_4$ ,  $\mathbb{F}_4$ ,  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , or  $\mathbb{F}_2[t]/(t^2)$ . Of these, the only ones that are local rings and are not fields are  $\mathbb{Z}_4$  and  $\mathbb{F}_2[t]/(t^2)$ . Note that both of these have the equivalent properties (1), (2), (3) of Proposition 4.7. Also note that if  $R = \mathbb{Z}_4$  or  $R = \mathbb{F}_2[t]/(t^2)$  there are exactly two irreducible GE polynomials of degree 2 in  $R[x]$ . (See Remark 3.6.) We will need this fact in the next proof.

In the next lemma, we find the set of lengths of  $x^6$ ; it will also be used as the base for an induction in the proposition to follow.

**Lemma 4.10.** *Suppose  $\mathfrak{m}^2 = 0$ . If  $|R| > 4$  then  $L(x^6) = \{2, 3, 4, 6\}$ ; if  $|R| = 4$  then  $L(x^6) = \{2, 4, 6\}$ .*

*Proof.* By the remarks after Proposition 4.6, it is enough to show that (a) if  $|R| > 4$  then  $3 \in L(x^6)$ , and (b) if  $|R| = 4$  then  $3 \notin L(x^6)$ .

Proof of (a): We first show there exist three nonzero elements  $a, b, c$  in  $\mathfrak{m}$  satisfying  $a + b + c = 0$ .

Suppose  $\text{char}(R/\mathfrak{m}) = 2$ . By Proposition 4.8, we know there are two distinct nonzero elements  $a$  and  $b$  in  $\mathfrak{m}$ . We must have  $a + b \neq 0$ , since otherwise  $a = -b = b$  by Proposition 4.7 (3), a contradiction. With  $c = -(a + b)$  we have  $a + b + c = 0$  for three nonzero elements  $a, b, c$ .

If, on the other hand,  $\text{char}(R/\mathfrak{m}) \neq 2$ , then by Proposition 4.7, there exists a nonzero element  $a \in \mathfrak{m}$  with  $2a \neq 0$ . Now set  $b = a$  and  $c = -2a$ . Then  $a + b + c = 0$  and all three elements are nonzero.

Now by Corollary 3.5, each of the polynomials  $x^2 + a$ ,  $x^2 + b$ , and  $x^2 + c$  is an irreducible GE polynomial. Since  $a + b + c = 0$  and  $\mathfrak{m}^2 = 0$ , the factorization  $(x^2 + a)(x^2 + b)(x^2 + c) = x^6$  shows that  $3 \in L(x^6)$ .

Proof of (b): Suppose  $|R| = 4$  and  $3 \in L(x^6)$ . Then there exists three irreducible, monic, nonconstant GE polynomials  $f_1, f_2, f_3$  whose product is  $x^6$ . Without loss of generality we have the following three cases for  $(\deg(f_1), \deg(f_2), \deg(f_3))$ :  $(4, 1, 1)$ ,  $(3, 2, 1)$ , and  $(2, 2, 2)$ . For the first two cases,  $\deg(f_1)$  is greater than  $\deg(f_2)$  and  $\deg(f_3)$ , so by Proposition 3.7,  $6 = \text{ord}(x^6) = \text{ord}(f_1 f_2 f_3) = \deg(f_2) + \deg(f_3) < 6$ , which is a contradiction.

For the last case, since, as noted in Remark 3.6, there are exactly two irreducible GE polynomials of degree 2 in  $R[x]$ , at least two  $f_i$  are the same, say  $f_1 = f_2$ , and thus, since  $\mathfrak{m}^2 = 0$ ,  $f_1 f_2 = x^4$ . But since  $f_1 f_2 f_3 = x^6$ , we have  $f_3 = x^2$ , a contradiction since  $f_3$  is irreducible. So  $3 \notin L(x^6)$ .  $\square$

**Proposition 4.11.** *Suppose  $\mathfrak{m}^2 = 0$ . For all  $n \geq 6$ ,  $|R| > 4$  if and only if  $n - 3 \in L(x^n)$ .*

*Proof.* If  $|R| > 4$  then by Lemma 4.10,  $3 \in L(x^6)$ , so there is a factorization of  $x^6$  into three irreducible polynomials. Multiplying this factorization by  $x^{n-6}$  gives a factorization of  $x^n$  of length  $n - 3$ . Therefore  $n - 3 \in L(x^n)$ .

Now assume  $|R| = 4$ . We show  $n - 3 \notin L(x^n)$  for  $n \geq 6$  (equivalently,  $n \notin L(x^{n+3})$  for  $n \geq 3$ ) by induction on  $n$ . By Lemma 4.10,  $3 \notin L(x^6)$ . Now assume  $k \notin L(x^{k+3})$  for some  $k \geq 3$ . We show  $k + 1 \notin L(x^{k+4})$ .

Suppose by way of contradiction that  $k + 1 \in L(x^{k+4})$ ; then there exist  $k + 1$  irreducible, monic, nonconstant GE polynomials  $f_1, f_2, \dots, f_{k+1}$ , whose product is  $x^{k+4}$ . At least one  $f_i$  must be linear, since otherwise  $k + 4 = \deg(x^{k+4}) = \sum_{i=1}^{k+1} \deg(f_i) \geq 2(k + 1)$ , which is impossible since  $k \geq 3$ . Furthermore, at least one  $f_i$  must be non-linear. Without loss of generality, let  $f_1$  be linear and  $f_{k+1}$  be non-linear. Then by Proposition 3.7 there exists an irreducible GE polynomial  $h$  such that  $f_{k+1} f_1 = hx$ . Therefore  $f_1 \cdots f_k = (f_{k+1} f_1) f_2 \cdots f_k = (hx) f_2 \cdots f_k$ . We now have  $h f_2 \cdots f_k = x^{k+3}$  which implies  $k \in L(x^{k+3})$ . This contradicts our assumption. Therefore  $n \notin L(x^{n+3})$  for  $n \geq 3$ , or equivalently,  $n - 3 \notin L(x^n)$ .  $\square$

The next two Lemmas do not depend on the cardinality of the local ring  $R$ .

**Lemma 4.12.** *Suppose  $\mathfrak{m}^2 = 0$ . For all  $n \geq 7$ ,  $3 \in L(x^n)$*

*Proof.* Let  $n \geq 7$ . Let  $m$  be a nonzero element of the maximal ideal  $\mathfrak{m}$ , let  $\ell$  be a positive integer, and consider the following three factorizations.

$$(x^\ell + m)(x^{\ell+1} - m)(x^{\ell+1} - mx + m) = x^{3\ell+2} \quad (4.2)$$

$$(x^\ell + m)(x^{\ell+2} - m)(x^{\ell+2} - mx^2 + m) = x^{3\ell+4} \quad (4.3)$$

$$(x^\ell + m)(x^{\ell+3} - m)(x^{\ell+3} - mx^3 + m) = x^{3\ell+6} \quad (4.4)$$

By Corollary 3.5, each polynomial on the left side of the three factorizations is irreducible. Assume  $n \geq 7$ . There are three cases:

$n \equiv 0 \pmod{3}$ : Set  $\ell = \frac{n-6}{3}$ ; then from equation (4.4),  $3 \in L(x^n)$ .

$n \equiv 1 \pmod{3}$ : Set  $\ell = \frac{n-4}{3}$ ; then from equation (4.3),  $3 \in L(x^n)$ .

$n \equiv 2 \pmod{3}$ : Set  $\ell = \frac{n-2}{3}$ ; then from equation (4.2),  $3 \in L(x^n)$ .

Therefore for any integer  $n \geq 7$ , we have  $3 \in L(x^n)$ .  $\square$

**Lemma 4.13.** *Suppose  $\mathfrak{m}^2 = 0$ . For any integer  $n \geq 7$ :*

- (1)  $\{3, 4, 5, \dots, n - 4\} \cup \{n - 2, n\} \subseteq L(x^n)$  if  $n$  is odd.
- (2)  $\{2, 3, 4, 5, \dots, n - 4\} \cup \{n - 2, n\} \subseteq L(x^n)$  if  $n$  is even.

*Proof.* Suppose  $n \geq 7$  and  $n$  is odd. If  $n = 7$ , then  $\{3, 5, 7\} \subseteq L(x^7)$  by Lemma 4.5. Thus we may assume  $n \geq 9$ . Again by Lemma 4.5,  $\{3, 5, 7, \dots, n-2, n\} \subseteq L(x^n)$ , so it remains to show that if  $k$  is even and  $4 \leq k \leq n-4$ , then  $k \in L(x^n)$ . If  $4 \leq k \leq n-4$ , then  $n-k+3 \geq 7$ , so by Lemma 4.12,  $3 \in L(x^{n-k+3})$ ; that is, there exists a factorization of  $x^{n-k+3}$  of length 3. Multiplying both sides of this factorization by  $x^{k-3}$  we have  $k \in L(x^n)$ . This proves (1).

Now suppose  $n$  is even and  $n \geq 8$ . By Lemma 4.5,  $\{2, 4, 6, \dots, n-2, n\} \subseteq L(x^n)$ . It remains to show that if  $k$  is odd and  $3 \leq k \leq n-4$ , then  $k \in L(x^n)$ . If  $3 \leq k \leq n-4$  then  $n-k+3 \geq 7$ . By Lemma 4.12,  $3 \in L(x^{n-k+3})$ . That is, there is a factorization of  $x^{n-k+3}$  into three irreducible polynomials. Multiplying both sides of this factorization by  $x^{k-3}$  show  $k \in L(x^n)$ .  $\square$

The following is the main result of this paper, along with Proposition 4.6 and Lemma 4.10. Note that the only difference the cardinality of  $R$  makes is in whether or not  $n-3 \in L(x^n)$ .

**Theorem 4.14.** *Suppose  $\mathfrak{m}^2 = 0$ . Let  $n$  be an integer with  $n \geq 7$ .*

*If  $|R| > 4$  then*

$$\begin{aligned} L(x^n) &= \{3, 4, 5, \dots, n-2\} \cup \{n\} \text{ if } n \text{ is odd, and} \\ L(x^n) &= \{2, 3, 4, 5, \dots, n-2\} \cup \{n\} \text{ if } n \text{ is even.} \end{aligned}$$

*If  $|R| = 4$  then*

$$\begin{aligned} L(x^n) &= \{3, 4, 5, \dots, n-4\} \cup \{n-2, n\} \text{ if } n \text{ is odd, and} \\ L(x^n) &= \{2, 3, 4, 5, \dots, n-4\} \cup \{n-2, n\} \text{ if } n \text{ is even.} \end{aligned}$$

*Proof.* Let  $n \geq 7$ . Regardless of the cardinality of  $R$ , by Lemmas 4.3 and 4.13, if  $n$  is odd,

$$\{3, 4, \dots, n-4\} \cup \{n-2, n\} \subseteq L(x^n) \subseteq \{1, 2, \dots, n\},$$

and if  $n$  is even,

$$\{2, 3, 4, \dots, n-4\} \cup \{n-2, n\} \subseteq L(x^n) \subseteq \{1, 2, \dots, n\}.$$

Since  $x^n$  is reducible,  $1 \notin L(x^n)$ . By Lemma 4.4,  $n-1 \notin L(x^n)$ , and  $2 \notin L(x^n)$  if  $n$  is odd. Finally, by Proposition 4.11,  $n-3 \in L(x^n)$  if and only if  $|R| > 4$ .  $\square$

**Example 4.15.** In  $\mathbb{Z}_{p^2}[x]$  where  $p$  is prime, we have

$$\begin{aligned} L(x^{10}) &= \{2, 3, 4, 5, 6, 7, 8, 10\} & \text{if } p > 2, \\ L(x^{10}) &= \{2, 3, 4, 5, 6, 8, 10\} & \text{if } p = 2. \end{aligned}$$

**Acknowledgment:** This article is a generalization of part of Daniel Kline's Master's Thesis [K] under the direction of Mark Rogers. The thesis work was inspired by the paper [FF] of Sophie Frisch and Christopher Frei, and a private email exchange with Sophie Frisch. The authors wish to thank the referee for several helpful suggestions and corrections.

## REFERENCES

- A1. Anderson, D. D. and Valdes-Leon, Silvia, *Factorization in commutative rings with zero divisors*, Rocky Mountain J. Math 26 (1996), 439–480.
- A2. Anderson, D. D. and Valdes-Leon, Silvia, *Factorization in commutative rings with zero divisors II*, Lecture Notes in Pure and Appl. Math, vol. 189, 197–219. Dekker, New York, 1997.
- A3. Ağargün, Ahmet G. and Anderson, D. D. and Valdes-Leon, Silvia, *Factorization in commutative rings with zero divisors III*, Rocky Mountain J. Math 31 (2001), 1–21.



FF. Frei, C. and Frisch, S., *Non-unique factorization of polynomials over residue class rings of the integers*, Comm. Algebra 39 (2011), no. 4, 1482-1490.

G. Geroldinger, A., *Sets of Lengths*, arXiv:1509.07462 [math.GR]

K. Kline, D., *Sets of Lengths over Residue Class Rings of the Integers*, Master's thesis, Missouri State University, 2011.

M. McDonald, Bernard, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. **28**, Marcel Dekker, New York, 1974

DEPARTMENT OF MATHEMATICS, MISSOURI STATE UNIVERSITY, SPRINGFIELD, MO 65897, USA

**Email address:** `rbelshoff@missouristate.edu`

DEPARTMENT OF MATHEMATICS, MILLIGAN COLLEGE, TN 37682, USA

**Email address:** `dbkline@milligan.edu`

DEPARTMENT OF MATHEMATICS, MISSOURI STATE UNIVERSITY, SPRINGFIELD, MO 65897, USA

**Email address:** `markrogers@missouristate.edu`